38. (Newly Added) A computer readable medium having computer-executable instructions for performing the steps recited in claim 1.

39. (Newly Added) A computer readable medium having computer-executable instructions for performing the steps recited in claim 14.

40. (Newly Added) A computer readable medium having computer-executable instructions for performing the steps recited in claim 26.

41. (Newly Added) A computer readable medium having computer-executable instructions for performing the steps recited in claim 31.

REMARKS

Claims 1-41 are now pending in the present application. The independent claims are Claims 1, 14, 18, 22, 26, and 31. Claims 9, 14, 16, 17, 24, and 25 have been amended while Claims 26-41 have been added to the application. The specification has been amended to include the serial number of a related pending application.

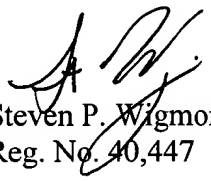
SUBMISSION OF ELECTRONIC PRE-GRANT PUBLICATION

Applicants respectfully submit that an electronic pre-grant publication containing the exact preliminary amendment has been electronically submitted to the Office today. The Applicants respectfully request that the submitted pre-grant publication be used instead of the originally filed paper version of the application.

CONCLUSION

Applicants respectfully submit that the above-styled continuation patent application, as amended, is in condition for examination and requests such action. If any issues remain that may be resolved by telephone, the Examiner is requested to call the undersigned at 404.572.4600.

Respectfully submitted,



Steven P. Wigmore
Reg. No. 40,447

King & Spalding
45th Floor
191 Peachtree Street, N.E.
Atlanta, Georgia 30303
404.572.4600
K&S Docket: 05456.105006

Version with markings to show changes made

Page 1, First Paragraph

The present application claims priority to provisional patent application entitled, "Intrusion Detection Fusion System of a Network Security System," filed on April 28, 2000 and assigned U.S. Application Serial Number 60/200,316. The present application is also related to non-provisional application entitled, "System and Method for Managing Security Events on a Network," (Attorney Docket No. 05456-105005) filed on April 27, 2001 and assigned U.S. Application Serial Number 09/844,448.

Page 15, First Full Paragraph

Referring now to Figure 2, the computer architecture for one exemplary embodiment of the present invention will be described. Figure 2 illustrates the System 20 for managing security information collected from one or more data sources. The security system 20 can comprise a fusion engine 22 that is linked to an event collector 24. The event collector 24 can comprise an event sink or device that can organize events received from multiple data sources in a logical manner. Further details of the event collector 24 are described in a related application entitled, "System and Method for Managing Security Events on a Network," (Attorney Docket No. 05456-105005) filed on April 27, 2001 and assigned U.S. Application Serial Number 09/844,448, the contents of which is hereby incorporated by reference.

9. (Once Amended) The method of claim 1, wherein the step of identifying relationships between two or more raw events further comprises the steps of:

associating each raw event with one or more rules that correspond [a rule which corresponds] with a type parameter of the [a] raw event; and

applying each rule to its associated group [one or more rules to groups] of raw events; and

determining if a computer attack or security breach has occurred based upon successful application of a rule.

14. (Once Amended) A method for determining relationships between two or more computer events, comprising the steps of:

receiving a plurality of raw events having a first set of parameters;

creating raw event storage areas based upon information received from a raw event classification database;

storing each event in an event storage area based upon an event type parameter;

comparing each raw event to data contained in a context database;

adjusting a priority parameter or leaving the priority parameter in tact for each raw event in response to the comparison to the context database;

associating [associate] each raw event with [a] one or more correlation events ;

applying one or more rules to each event based upon the correlation event associations; and

generating a mature correlation event message in response to each successful application of a rule.

16. (Once Amended) The method of claim 14, wherein the context database comprises any one of vulnerability values, computer event frequency values, [and] source and destination zone values, and detector zone values.

17. (Once Amended) The method of claim 14, wherein the raw event classification database comprises tables that include information that categorizes raw events based on any one of the following: how an activity indicated by a raw event may impact one or more target computers, how many target computers [that] may be affected by an activity indicated by a raw event, and how activities indicated by respective raw events gain access to one or more target computers.

24. (Once Amended) The fusion engine of claim 22, wherein the context database comprises any one of vulnerability values, computer event frequency values, [and] source and destination zone values, and detector zone values.

25. (Once Amended) The fusion engine of claim 22, wherein the raw event classification database comprises tables that include information that categorizes raw events based on any one of the following: how an activity indicated by a raw event may impact one or more target computers, how many target computers [that] may be affected by an activity indicated by a raw event, and how activities indicated by respective raw events gain access to one or more target computers.